Exhibit 2

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

District of New Jersey

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
THE REAL PROPERTY AND RESIDENCE AT [redacted] NEW JERSEY; 2016 BLACK MERCEDES-BENZ C300 BEARING [redacted]; 2021 WHITE MERCEDES-BENZ GLE BEARING [redacted]; and THE PERSON OF OLUWASEUN ADEKOYA

Case No. 23-16155, 23-16156, 23-16157, 23-16158

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachments A-1, A-2, A-3, and A-4

located in the _____ District of New Jersey, there is now concealed *(identify the person or describe the property to be seized)*:

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*;

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1349, 18 U.S.C. § 1344, and 18 U.S.C. § 1028A	Conspiracy to commit bank fraud; aggravated identity theft

The application is based on these facts:

See Attachment C

- ☐ Continued on the attached sheet.
- ☑ Delayed notice of 30 days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Spenser Warren, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 12/08/2023

Jose R. Almonte
Judge's signature

City and state: District of New Jersey

Hon. José R. Almonte
Printed name and title

ATTACHMENT C

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

THE MATTER OF THE SEARCH OF:	:	Hon. José R. Almonte
THE REAL PROPERTY AND RESIDENCE AT [redacted] NEW JERSEY;	:	Mag. No. 23-16155
2016 BLACK MERCEDES-BENZ C300 BEARING [redacted]	:	Mag. No. 23-16156
2021 WHITE MERCEDES-BENZ GLE [redacted]; and	:	Mag. No. 23-16157
THE PERSON OF OLUWASEUN ADEKOYA.	:	Mag. No. 23-16158
	:	**Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR WARRANTS TO SEARCH AND SEIZE

I, Spenser Warren, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premise, vehicles, and person identified in Attachments A-1 through A-4, and to seize evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1349 and 1344 (conspiracy to commit bank fraud) and 18 U.S.C. § 1028A (aggravated

identity theft) (collectively the "Subject Offenses"), as further described in Attachments B-1 through B-4, respectively.

2. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since March 2020. I am currently assigned to the Albany Field Office, investigating white collar violations, including complex financial crime. Prior to my FBI employment, I graduated from the Delaware State Police Academy in 2016 and served as a police officer in the states of Delaware and New Jersey for three years. I hold a bachelor's degree in human resources management and a Master of Business Administration (MBA) degree. I have been a certified professional in human resources (SHRM-CP) for approximately five years and a certified fraud examiner (CFE) for approximately three years. Since joining the FBI, I have received training on the proper techniques for investigating financial crimes, including the use of surveillance, undercover activities, financial analysis, and the application for and execution of search and arrest warrants.

3. As the case agent, I am fully familiar with the facts of this case. The facts in this affidavit come from my personal observations, review of evidence and the FBI case file, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Where statements of others are related in this affidavit, they are related in substance and in part.

4. As set forth below, there is probable cause to believe that Oluwaseun ADEKOYA, together with David DANIYAN, Jerjuan JOYNER, Akeem BALOGUN, Gaysha KENNEDY, Victor BARRIERA, Lesley LUCCHESE, Danielle CAPPETTI, D[redacted] P[redacted] collectively "the Targets", and others, have committed the Subject Offenses and that evidence, fruits, and instrumentalities of the Subject Offenses will be found on the person and within the properties to be searched, as set forth in Attachments B-1 through B-4.

THE PERSON AND PROPERTIES TO BE SEARCHED

5. Oluwaseun ADEKOYA was born on [redacted] in Lagos, Nigeria. ADEKOYA is approximately 6 feet tall, weighing approximately 190 pounds. ADEKOYA has brown eyes, black hair, and a dark skin complexion.

6. [redacted] New Jersey [redacted] is the residence of ADEKOYA and his spouse A[redacted] C[redacted] The area to be searched includes any garage space or storage units located within the apartment building utilized or controlled by ADEKOYA, and any closed or open containers therein. [redacted] is located within [redacted], which is a high-rise luxury apartment rental community that offers approximately 314 separate studio, one, and two bedroom apartments for lease. The building appears to be approximately 15 stories tall with 24-hour security, a rooftop pool, a grand plaza with restaurants and retail stores, a fitness center, a lounge, and an underground parking garage, per the property's website. Based on publicly accessible floor plans, [redacted] likely contains a living room, a kitchen, a laundry room, closet space, at least

one bedroom, and at least one bathroom. A photograph of [redacted]

[redacted]

7. ADEKOYA is the titled owner of a 2016 black Mercedes-Benz C300 bearing [redacted] ("C300"). The C300 is used by ADEKOYA and his wife, A[redacted] T[redacted] O[redacted]

8. ADEKOYA is the lessee of a 2021 white Mercedes-Benz GLE bearing [redacted] ("GLE"). The GLE is used by ADEKOYA and his wife, A[redacted] T[redacted] O[redacted]

INTRODUCTION

9. This search warrant arises out of a federal investigation concerning conspiracy to commit bank fraud and other federal fraud offenses, committed by the Targets in the Northern District of New York and elsewhere. More specifically, as further set forth below, since at least December 1, 2021, the Targets have devised and executed a scheme to defraud various credit unions, the accounts of which were insured by National Credit Union Share Insurance Fund, targeted primarily by exploiting the Co-op Solutions Shared Branch network (the "Shared Branch network").

10. The Shared Branch network enables the customers of a Shared Branch network member credit union to perform a range of transactions at branches of other Shared Branch network member credit unions. This allows member credit unions to serve their customers in diverse geographic locations, even when the customers move or travel.

11. For example, among other transactions, the Shared Branch network allows the customers of one member credit union to withdraw funds from their account at a branch of another member credit union by presenting a photo identification and providing their account number and the last four digits of their Social Security number.

12. To exploit the Shared Branch network, participants in the scheme, including Targets ADEKOYA and DANIYAN, obtain the names, account numbers, and last four digits of the Social Security numbers for customers of member credit unions. That information is provided to other participants in the scheme, including Targets BARRIERA, CAPPETTI, LUCCHESE, and P[redacted] who impersonate the customers at other member credit unions; present fictitious driver's licenses in the customers' names but bearing the impersonating Target's photograph; and fraudulently withdraw funds from the customers' accounts. Other participants in the scheme, including Targets JOYNER, BALOGUN, and KENNEDY, have driven the participants impersonating customers to numerous credit unions in certain geographic areas within the Northern District of New York and throughout the United States and were paid with proceeds of the fraudulent transactions. Through investigation we have identified more than 200 successful fraudulent transactions that were part of the Targets' scheme and conspiracy. These took place at credit unions in the Northern District of New York and all over the country, resulting in losses exceeding $900,000.

PROBABLE CAUSE

13. On or about May 9, 2022, CAP COM Federal Credit Union ("CAP COM"), headquartered in Albany, New York, in the Northern District of New York, became aware of a series of fraudulent cash withdrawals being conducted at CAP COM branches in the Albany, New York region. The cash withdrawals were similar in that they exploited the Shared Branch network.

14. CAP COM determined that between May 7, 2022 and May 9, 2022, at least ten fraudulent cash withdrawals had been conducted at ten separate CAP COM branches utilizing the Shared Branch network. The ten withdrawals equated to approximately $48,500 in losses from five unique accounts, all of which were assigned to customers of Seasons Federal Credit Union ("Seasons FCU") of Meriden, Connecticut.

15. Review of CAP COM surveillance footage showed a female, later identified as LUCCHESE, conducting eight separate cash withdrawals in the name of four Seasons FCU customers, including individuals with initials [redacted]. On each occasion, a fictitious Connecticut driver's license was provided to enable the withdrawal, as documented by the tellers on the transaction receipts.

16. In addition, review of surveillance footage showed a male conducting two separate cash withdrawals in the name of one Seasons FCU customer, with initials [redacted]. A fictitious Connecticut driver's license was provided to enable the withdrawals, as documented by the teller on the transaction receipts.

17. [redacted] for Seasons FCU, subsequently confirmed to me that these transactions were fraudulent.

18. On May 19, 2022, CAP COM identified additional suspicious activity as BARRIERA conducted suspected fraudulent cash withdrawals in the Albany, New York region using the Shared Branch network. CAP COM investigators shared a photograph of BARRIERA with their branch staff and a description of a vehicle that had been dropping BARRIERA off at various CAP COM branches. On May 19, 2022, a teller at the CAP COM branch located at 219 Ontario Street, Cohoes, New York branch identified BARRIERA attempting a Shared Branch cash withdrawal in his teller lane. Cohoes Police Department was subsequently contacted.

Cohoes Police Department Arrest of BARRIERA on May 19, 2022

19. On May 19, 2022, Cohoes Police Department, in the Northern District of New York, encountered BARRIERA at the 219 Ontario Street CAP COM branch and interviewed BARRIERA. BARRIERA initially represented himself to Cohoes Police Department as [redacted] of New Hampshire, from whose account BARRIERA was attempting to withdraw money. BARRIERA was in possession of a New Hampshire driver's license bearing some of [redacted] personal identifiers, but the license number was fictitious and a photograph of BARRIERA's face had been printed on the license. CAP COM staff advised Cohoes Police Department that approximately two hours prior to BARRIERA representing himself as [redacted] of New Hampshire, BARRIERA had represented himself as [redacted] of New Hampshire at a CAP COM branch located at 4 Winners

Circle, Albany, New York and successfully withdrew $5,000 via the Shared Branch network from [redacted] account. BARRIERA was subsequently arrested by Cohoes Police Department and did not reveal his true name and date of birth until after being taken into custody.

20. At the time of BARRIERA's arrest, he was in possession of a gray-colored cellular phone contained within a red-colored Samsung protective case. This phone was seized by Cohoes Police Department and documented as seized evidence subsequent to arrest.

Cohoes Police Department Arrest of DANIYAN and KENNEDY on May 19, 2022

21. CAP COM investigators had utilized surveillance footage to determine that a silver Nissan Rogue bearing a New York registration plate had been dropping BARRIERA off at the area credit unions. This information was communicated to Cohoes Police Department at the time of their dispatch and a Cohoes Police Department officer located a vehicle matching this description leaving the vicinity of 219 Ontario Street as he pulled into the CAP COM branch to interdict BARRIERA. This officer turned around and conducted a traffic stop while other officers encountered BARRIERA. The traffic stop resulted in identification of the driver as KENNEDY and the back seat passenger, who represented himself as [redacted] (later identified by Cohoes Police Department as "Bamikole Laniyan," but whom FBI has subsequently determined to actually be DANIYAN).

22. At the time of the traffic stop, DANIYAN repeatedly reached for a black duffel bag near his feet in the backseat. Both occupants were asked to

exit the vehicle and both occupants verbally consented to a search of the vehicle. Search of the vehicle revealed a fictitious Nigerian passport located within DANIYAN's backseat wingspan, bearing DANIYAN's photograph with the name [redacted] and date of birth [redacted]. Further search of the vehicle revealed a large sum of United States currency, a folder containing credit union customers' personal identifying information ("PII"), and five cellular devices (four located in the backseat and one in the front seat).

23. Both KENNEDY and DANIYAN were detained and transported back to the Cohoes Police Department for further questioning. KENNEDY, the registered owner of the vehicle, advised Cohoes Police Department in sum and substance that she dropped a male passenger off in the direction of 219 Ontario Street and she was an Uber driver from New York City and didn't know the two male passengers. Ultimately, BARRIERA, KENNEDY, and DANIYAN (under the name "Bamikole Laniyan") were charged with several felonies under New York State law.

June 9, 2022 Federal Search Warrant for Phones Seized from BARRIERA, KENNEDY, and DANIYAN

24. On June 9, 2022, I swore out an application and affidavit in support of a search warrant in the U.S. District Court for the Northern District of New York, pursuant to which the Court issued a federal search warrant for six cellular devices that had been seized by Cohoes Police Department in Cohoes, New York on May 19, 2022.

25. At the time of swearing to this search warrant, I had become aware of approximately 40 fraudulent cash withdrawals exploiting the Shared Branch

network between April 22, 2022 and May 26, 2022. I was aware of approximately 25 identity theft victims who banked with Seasons Federal Credit Union of Meriden, Connecticut, Sunmark Federal Credit Union of Albany, New York, Triangle Credit Union of Nashua, New Hampshire, and Robins Financial Credit Union of Warner Robins, Georgia. The known loss amount at that time was approximately $184,100.

26. Surveillance footage received from various involved credit unions indicated that BARRIERA was responsible for at least 12 of the known fraudulent transactions, impersonating at least seven different victims, dating back to at least January 27, 2022. Surveillance from Suffolk Federal Credit Union appeared to show DANIYAN assisting an unidentified female in conducting a $5,000 fraudulent transaction at 691 Route 25A, Miller Place, New York on May 4, 2022.

27. On January 27, 2022, BARRIERA did not exploit the Shared Branch network, but actually withdrew money from the victim's own credit union. BARRIERA impersonated victim [redacted] using a fictitious New Jersey driver's license and was able to withdraw $15,000 from the victim's home equity line of credit via cash advances in three separate transactions at three separate Suffolk Federal Credit Union branches within two hours.

28. For the purposes of this search warrant, the cellular devices searched pursuant to the June 9, 2022 search warrant are identified as follows:

a. Phone 1B2, or Phone #1, was seized from BARRIERA's person by Cohoes Police Department. Phone #1 was a Samsung Galaxy A32. Phone #1's Mobile Station Integrated Services Digital Network (MSISDN) number, also known as the assigned phone number, was [redacted]4654. Phone #1 was later logged into FBI evidence as Evidence Item 1B2.

b. Phone 1B3, or Phone #2, was seized from the driver area of the vehicle searched by Cohoes Police Department where KENNEDY was seated. Phone #2's MSISDN number was [redacted]6662. Phone #2 was later logged into FBI evidence as Evidence Item 1B3.

c. Phone 1B4, or Phone #3, was seized from the backseat area of the vehicle searched by Cohoes Police Department where DANIYAN was seated. Phone #3 was a Nokia C01 Plus. Phone #3's MSISDN number was [redacted]7932. Phone #3 was later logged into FBI evidence as Evidence Item 1B4.

d. Phone 1B5, or Phone #4, was seized from the backseat area of the vehicle searched by Cohoes Police Department where DANIYAN was seated. Phone #4 was a T-Mobile RVVL 4G. Phone #4's MSISDN number was [redacted]7895. Phone #4 was later logged into FBI evidence as Evidence Item 1B5.

e. Phone 1B6, or Phone #5, was seized from the backseat area of the vehicle searched by Cohoes Police Department where DANIYAN was seated. Phone #5 was an Apple iPhone. Phone #5's MSISDN

number was [redacted]0395. Phone #5 was later logged into FBI evidence as Evidence Item 1B6.

f. Phone 1B7, or Phone #6, was seized from the backseat area of the vehicle searched by Cohoes Police Department where DANIYAN was seated. Phone number [redacted]4337 was taped to the backside of Phone #6. Phone #6 was heavily damaged, preventing FBI from conducting a successful data extraction. Phone #6 was later logged into FBI evidence as Evidence Item 1B7.

Evidence Contained Within Phone 1B2

29. On June 15, 2022, FBI Computer Scientist Alejandro Vargas performed a mobile device extraction of Phone 1B2 and prepared a Cellebrite software report for my forensic review.

30. Evidence obtained from Phone 1B2 established that the phone was used by BARRIERA. This included numerous "selfie" photographs of BARRIERA, personal emails, communications with BARRIERA's landlord and girlfriend, communications about drug usage, and several photographs of drugs and a gun in what appears to be BARRIERA's apartment. Additionally, Phone 1B2 contains a large amount of identity theft information, to include numerous photographs of victim names, date of births, social security numbers, bank account numbers, phone numbers, email addresses, spousal information, bank account balances, and fictitious driver's licenses where BARRIERA's face was paired with victim's PII. This information, coupled with surveillance footage subsequently obtained from credit unions, led me to

believe that BARRIERA was involved in at least 45 separate fraudulent cash withdrawals, an account opening, and an account takeover, impersonating at least ten different victims dating back to at least December 2021.

31. Two particular phone numbers of interest were saved in Phone 1B2, and with which BARRIERA communicated about the conspiracy: [redacted] 4337 and [redacted] 7932, which were saved as "Boss Man Jame$$" and "Boss Jame", respectively. The phone number associated with "Boss Man Jame$$" was taped to the backside of Phone 1B7, which had been inaccessible until October 2, 2023 due to extensive damage. The phone number associated with "Boss Jame" was the MSISDN linked to Phone 1B4.

32. Based upon call detail records obtained from T-Mobile, Phone 1B2 received calls or text messages from Phone 1B4, Phone 1B5, and Phone 1B7. Phone 1B2 sent calls or text messages to Phone 1B4 and Phone 1B7.

Evidence Contained Within Phone 1B4

33. FBI Computer Scientist (CS) Alejandro Vargas obtained a mobile device extraction of Phone 1B4 on September 22, 2022 once new software had been published, enabling a successful extraction. CS Vargas prepared a Cellebrite software report for my forensic review.

34. The user of Phone 1B4, believed to be DANIYAN, had a text message dialogue with the user of phone number [redacted] 6662, the MSISDN linked to Phone 1B3. Records obtained from T-Mobile showed the phone number linked to Phone 1B3 was registered to [redacted], believed to be KENNEDY's mother. DANIYAN saved KENNEDY's contact as "KEYS ALISHA".

The text message dialogue between DANIYAN and KENNEDY appeared to discuss payment and plans to drive up to the Albany, New York area on the day that Cohoes Police Department and Colonie Police Department effected their arrests. Two excerpts from the text message dialogue are displayed below:

From: KEYS ALISHA (Phone 1B3)	To: [redacted] 7932 (Phone 1B4)	5/16/2022 @ 10:16 PM	Good night! We talked 1500-2000 when we met! I understand today was bad/ slow so let me know going forward.... I appreciate it it's nothing no hard work but I need to know going forward Have a good night talk to you tomorrow
From: [redacted] 7932 (Phone 1B4)	To: KEYS ALISHA (Phone 1B3)	5/16/2022 @ 10:31 PM	I told you on a good day you can make up to 1500 to 2k I did not say everyday , sometimes it gets worse but we always make sure we secure

			something by all means necessary so don't be ahead of yourself . Night Night

From: [redacted] 7932 (Phone 1B4)	To: KEYS ALISHA (Phone 1B3)	5/19/2022 @ 6:42 AM	I told you Vic will do most of the driving
From: [redacted] 7932 (Phone 1B4)	To: KEYS ALISHA (Phone 1B3)	5/19/2022 @ 6:45 AM	I'm by Chipotle on myrtle . Let me know what you wanna do . I'm in the rain
From: [redacted] 7932 (Phone 1B4)	To: KEYS ALISHA (Phone 1B3)	5/19/2022 @ 6:49 AM	Common now tell me something I'm in the rain are you going with us Yes or No ?
From: [redacted] 7932 (Phone 1B4)	To: KEYS ALISHA (Phone 1B3)	5/19/2022 @ 6:52 AM	What's going on with you ? You can just text me and let me know what you want to do instead of being incommunicado

From: [redacted] 7932 (Phone 1B4)	To: KEYS ALISHA (Phone 1B3)	5/19/2022 @ 7:00 AM	You're better than that girl. Ignoring my text and calls by hanging up on me is big time disrespectful . Don't like that . I won't do such a thing to you better yet, anyone . Smh
From: KEYS ALISHA (Phone 1B3)	To: [redacted] 7932 (Phone 1B4)	5/19/2022 @ 7:01 AM	I'm just waking ok I don't have time to read this shit
From: [redacted] 7932 (Phone 1B4)	To: KEYS ALISHA (Phone 1B3)	5/19/2022 @ 7:02 AM	What do you want to do should I wait for you
From: [redacted] 7932 (Phone 1B4)	To: KEYS ALISHA (Phone 1B3)	5/19/2022 @ 7:04 AM	Do you want me to stick around for you
From: [redacted] 7932 (Phone 1B4)	To: KEYS ALISHA (Phone 1B3)	5/19/2022 @ 7:04 AM	Yes or no
From: KEYS ALISHA	To: [redacted] 7932	5/19/2022 @ 8:20 AM	Hello

(Phone 1B3)	(Phone 1B4)		
From: [redacted] 7932 (Phone 1B4)	To: KEYS ALISHA (Phone 1B3)	5/19/2022 @ 8:32 AM	I'll come over by we'll do it in NY
From: [redacted] 7932 (Phone 1B4)	To: KEYS ALISHA (Phone 1B3)	5/19/2022 @ 9:23 AM	I'm here
From: [redacted] 7932 (Phone 1B4)	To: KEYS ALISHA (Phone 1B3)	5/19/2022 @ 9:25 AM	I'm on Atlantic on Thomas Boyland
From: KEYS ALISHA (Phone 1B3)	To: [redacted] 7932 (Phone 1B4)	5/19/2022 @ 9:25 AM	I'm on my way

35. MSISDN linked to Phone 1B2 was saved to DANIYAN's Phone 1B4 with contact name "BRONX VIC". A text message dialogue occurred between the two devices on April 27, 2022, where DANIYAN sent BARRIERA photographs of two identity theft victims' signatures on legal documents and instructed BARRIERA to practice forging the signatures. BARRIERA subsequently forwarded these photographs to JOYNER at a phone number known to be used by JOYNER. BARRIERA had saved JOYNER in Phone 1B2 as "Bro Jay $$". BARRIERA complained to JOYNER, in part, that, "boss man send me two signatures... to practice... they both are hard and being sick the

way I am right now I cannot concentrate very well..." JOYNER later responded, "Ok cool."

36. Based upon call detail records obtained from T-Mobile, Phone 1B4 received calls or text messages from Phone 1B2, Phone 1B3, Phone 1B5, and Phone 1B7. Phone 1B4 sent calls or text message to Phone 1B2, Phone 1B3, Phone 1B5, and Phone 1B7.

Evidence Contained Within Phone 1B5

37. CS Alejandro Vargas obtained a mobile device extraction of Phone 1B5 on June 17, 2022 and prepared a Cellebrite software report for my forensic review.

38. The user of Phone 1B5, believed to be DANIYAN, displayed connections to the conspiracy. This included photographs of text message dialogues between BARRIERA and the user of Phone 1B7, also believed to be DANIYAN. In one text message dialogue, photographed on February 2, 2022 by Phone 1B5, "VIC BRONX" writes to DANIYAN on Phone 1B7 "I hope whatever we using tomorrow when I walk in that I'm not a black man being 75 years old please make it be more less about my age". "VIC BRONX" received the following response, "Bro, Why now ? You shouldn't have led me on if you don't want to work and I personally wouldn't give a F if you've told me you not going. Vic this is your 3rd time of doing this because you're not the one spending your money to put this together and if I'm holding on to some of your cash to put our work together I believe you won't act as such . My question to you is, why can't you tell me how you feel before they put things together ? You told me you

bought yourself a shirt and tie for this job and apparently you gave me the go ahead to buy your ticket..."

39. Phone 1B5 also contained photographs of fraudulent checks and photographs of individuals which appear to have been taken for the purpose of creating fictitious identifications. In my training and experience, it is typical for the fraudulent masterminds to distance themselves from the fraudulent transactions by employing individuals, such as BARRIERA, to conduct the fraudulent transactions. Thus, for example, there is a photograph of BARRIERA's face on Phone 1B5, captured on January 24, 2022.

40. Based upon call detail records obtained from T-Mobile, Phone 1B5 received calls or text messages from Phone 1B4, Phone 1B6, and Phone 1B7. Phone 1B5 sent calls or text messages to Phone 1B2 and Phone 1B4.

Evidence Contained Within Phone 1B6

41. CS Alejandro Vargas obtained a mobile device extraction of Phone 1B6 on June 21, 2022 and prepared a Cellebrite software report for my forensic review.

42. Phone 1B6 contains attribution to DANIYAN. This includes selfie photographs, photographs and videos of DANIYAN with his family, communications with DANIYAN's family members, and funeral plans for DANIYAN's mother. Additionally, the phone contains research on credit unions that were targeted, research on the physical appearance of various state's driver's licenses, videos of prospective bank runner's faces including one that was contained on Phone 1B5, videos of fictitious driver's licenses with

BARRIERA's face printed on them, and videos of the same signatures that BARRIERA was asked to forge by the user of Phone 1B4.

43. Phone 1B6 contains a WhatsApp conversation between DANIYAN and a WhatsApp account associated with the phone number assigned to Phone 1B5. The Phone 1B5 WhatsApp account was named "Tony" with an alternate name of "BIG DADDY". From November 2021 to May 2022, the two accounts share research on credit unions to exploit, identity theft victim information, victim account balances, photographs of what is believed to be DANIYAN's wife's Nigerian passport, rows of what appear to be fraudulent credit cards, Nigerian bank account numbers, and photographs of prospective bank runners.

44. Based upon call detail records obtained from T-Mobile, Phone 1B6 did not receive calls or text messages from any of the other conspirators' devices. Phone 1B6 only sent calls or text messages to Phone 1B5.

Okaloosa County Sheriff's Office Arrest of DANIYAN, LUCCHESE, and BALOGUN on October 27, 2022

45. On November 2, 2022, FBI Special Agent Heather Johnson of FBI Jacksonville advised me of the arrest of DANIYAN, LUCCHESE, and BALOGUN by Escambia County Sheriff's Office and Okaloosa County Sheriff's Office in the Pensacola, Florida area. LUCCHESE had been identified as a subject of interest by Eglin Federal Credit Union, a member of the Shared Branching network. On October 25, 2022, LUCCHESE's image had been captured on Eglin Federal Credit Union security cameras, impersonating at least six different residents of Utah using fictitious government identifications at various

credit union branches to conduct cash withdrawals totaling approximately $50,000. Escambia County Sheriff's Office and Okaloosa County Sheriff's Office obtained video footage from a local CVS pharmacy showing the rental vehicle that had been identified as associated with LUCCHESE during her fraudulent transactions. The vehicle had been rented by BALOGUN.

46. The vehicle was later located at a Tom Thumb gas station in Pensacola, Florida by Escambia County Sheriff's Office Investigator Greg Goult. At the time of encounter, BALOGUN had just finished pumping gas and was about to enter the driver's seat. DANIYAN was seated in the front passenger's seat and LUCCHESE was seated in the back seat. Investigator Goult seized DANIYAN's gray-colored T-Mobile REVVLV Android cell phone from DANIYAN's person as DANIYAN was detained and subsequently arrested. Other investigators seized BALOGUN's black-colored Samsung cell phone, contained within a worn, gray-colored case, from BALOGUN's person as BALOGUN was detained and subsequently arrested. Both phones were turned over to the Okaloosa County Sheriff's Office, who were leading the investigation. The phones were individually packaged and sealed in evidence bags and were stored in a secured evidence storage facility under case number OCSO22OFF015493 at the Okaloosa County Sheriff's Office, 50 2nd Street, Shalimar, Florida 32579.

47. Following advisement of their Miranda rights, LUCCHESE, BALOGUN, and DANIYAN provided information regarding the conspiracy to investigators. LUCCHESE stated that she was a homeless resident of New York

and DANIYAN would provide her with fictitious identification cards. DANIYAN stated that he took orders from others who directed him on what credit unions to go to. BALOGUN would drive to the credit unions and DANIYAN would provide fictitious identification cards to LUCCHESE and instruct her on making account withdrawals. Following each transaction, DANIYAN claimed he would keep approximately $1,000 for himself and provide approximately $500 to LUCCHESE and BALOGUN. DANIYAN delivered the rest of the money to unknown others. DANIYAN informed the investigators that they had recently traveled to the state of Washington to commit similar crimes. BALOGUN admitted that he had been in Washington State making trips to credit unions with DANIYAN shortly before they traveled to Florida.

48. The vehicle operated by BALOGUN was subsequently towed incident to arrest and Okaloosa County Sheriff's Office Investigator Richard Cooper swore to a vehicle search warrant on November 1, 2022 before the Honorable Judge Terrance R. Ketchel, Circuit Judge for the First Judicial Circuit of Florida. Upon receipt of the vehicle search warrant, three additional cellular devices were seized from the vehicle. The additional devices included a black-colored AT&T flip-style phone located on the dashboard area above the glove compartment on the passenger's side of the vehicle, where DANIYAN was seated. Another phone seized included a gray-colored T-Mobile Android phone with AI Dual Camera technology, located on the dashboard area above the glove compartment on the passenger's side of the vehicle, where DANIYAN was seated. Another phone seized included a black-colored Samsung Android

phone with a multi-colored back cover, located inside LUCCHESE's purse on the driver's side backseat. All three phones were individually packaged and sealed in evidence bags and submitted to a secured evidence storage facility under case number OCSO22OFF015493 at the Okaloosa County Sheriff's Office, 50 2nd Street, Shalimar, Florida 32579.

49. On November 8, 2022, I swore out an application and affidavit in support of a search warrant in the U.S. District Court for the Northern District of Florida, pursuant to which the Court issued a federal search warrant for five cellular devices that had been seized by Okaloosa County Sheriff's Office between October 27 and November 1, 2022.

50. For the purposes of this search warrant, the cellular devices described during the November 8, 2022 search warrant are identified as follows:

a. Phone #1B22, or Phone #7, was seized from DANIYAN's person by Escambia County Sheriff's Office. Phone #7 was a T-Mobile REVVL V Android cell phone. Phone #7's MSISDN's were [redacted]0436 and [redacted]4013. Phone #7 was later logged into FBI evidence as Evidence Item 1B22.

b. Phone #1B21, or Phone #8, was seized from BALOGUN's person by Escambia County Sheriff's Office. Phone #8 was a Samsung Galaxy A20. Phone #8's MSISDN's were [redacted]9162, [redacted]4654, and [redacted]5762. Phone #8 was later logged into FBI evidence as Evidence Item 1B21.

c. Phone 1B23, or Phone #9, was seized from a location of the vehicle in which DANIYAN sat by Okaloosa County Sheriff's Office. Phone #9 was a AT&T Cingular Flip 2. Phone #9's MSISDN's was [redacted]9210. Phone #9 was later logged into FBI evidence as Evidence Item 1B23.

d. Phone 1B24, or Phone #10, was seized from a location of the vehicle in which DANIYAN sat by Okaloosa County Sheriff's Office. Phone #10 was a T-Mobile REVVL V. Phone #10's MSISDN was [redacted]3325. Phone #10 was later logged into FBI evidence as Evidence Item 1B24.

e. Phone 1B25, or Phone #11, was seized from LUCCHESE's purse, located within the vehicle by Okaloosa County Sheriff's Office. Phone #11 was a Samsung Galaxy A12. Phone #11's MSISDN was [redacted]5048. Phone #11 was later logged into FBI evidence as Evidence Item 1B25.

Evidence Contained Within Phone 1B21

51. On November 18, 2022, FBI Computer Scientist Alejandro Vargas performed a mobile device extraction of Phone 1B21 and prepared a Cellebrite software report for my forensic review.

52. Evidence obtained from Phone 1B21 established that the phone was used by BALOGUN. T-Mobile records show that the MSISDN assigned to Phone 1B21 was registered to BALOGUN and the contents of Phone 1B21

included BALOGUN's identification documents, selfie photographs, and logins to personal accounts.

53. Waze app data located on Phone 1B21 showed BALOGUN navigating to credit unions across Illinois, Florida, and Washington state that through my investigation I have learned were victimized by DANIYAN, BALOGUN, LUCCHESE, and P[redacted] from September 15 to October 26, 2022. I have also learned that BALOGUN deposited thousands of dollars in cash via Bank of America ATM deposits within the vicinity of the fraudulent withdrawals – activity that was out of the ordinary from BALOGUN's previous account activity. In my training and experience, this is consistent with BALOGUN being paid in cash out of the proceeds of fraudulent bank transactions. In addition, based on a chronological analysis of Phone 1B21 activity paired with credit union records, there were numerous occasions wherein BALOGUN was querying the next credit union to travel to prior to the bank runner leaving the credit union where BALOGUN had just dropped them off.

54. Based upon call detail records obtained from T-Mobile, Phone 1B21 received calls or text messages from Phone 1B22. Phone 1B21 sent calls or text messages to Phone 1B22.

Evidence Contained Within Phone 1B23

55. On November 23, 2022, FBI Computer Scientist Alejandro Vargas performed a mobile device extraction of Phone 1B23 and prepared a Cellebrite software report for my forensic review.

56. Evidence obtained from Phone 1B23 established that the phone was used by DANIYAN. Communications show that DANIYAN had intimate knowledge of the fraud conspiracy and communicated with both LUCCHESE and P[redacted] while they were conducting fraudulent credit union cash withdrawals. Evidence derived from Phone 1B22 showed that DANIYAN was directing LUCCHESE's and P[redacted] actions. Additionally, DANIYAN used this device to communicate with his other devices, including Phone 1B22.

57. Based upon call detail records obtained from T-Mobile, Phone 1B23 received calls or text messages from Phone 1B22 and Phone 1B25. Phone 1B23 sent calls or text messages to Phone 1B25.

Evidence Contained Within Phone 1B24

58. On November 23, 2022, FBI Computer Scientist Alejandro Vargas performed a mobile device extraction of Phone 1B24 and prepared a Cellebrite software report for my forensic review.

59. Evidence obtained from Phone 1B24 established that the phone was used by DANIYAN. DANIYAN's known family members are saved in Phone 1B24's contacts and are frequently communicated with. Additionally, DANIYAN text messaged phone number [redacted]3242 on May 25, 2022. It appeared that the message was likely spam, impersonating CitiBank, however DANIYAN replied, [redacted]7895 JAMES TONY." This further indicated that Phone 1B5 was owned and used by DANIYAN, primarily as a personal device.

60. Further, based upon call detail records obtained from T-Mobile, Phone 1B24 did not receive calls or text messages from any other phone

number seized in Florida. Phone 1B24 only sent calls or text messages to Phone 1B22. This pattern of activity is indicative in my training and experience of DANIYAN attempting to separate himself from the fraudulent activity by maintaining his personal life on a separate cellular device.

Evidence Contained Within Phone 1B25

61. On November 18, 2022, FBI Computer Scientist Alejandro Vargas performed a mobile device extraction of Phone 1B25 and prepared a Cellebrite software report for my forensic review.

62. Evidence obtained from Phone 1B25 established that the phone was used by LUCCHESE. The phone contained logins to LUCCHESE's personal accounts, LUCCHESE's financial information, selfie photographs, and text messages and emails with associates and conspirators.

63. For example, in Phone 1B25, LUCCHESE saved phone number [redacted]9210, the number linked to Phone 1B23, as "Nigerian". On October 18, 2022, DANIYAN advised LUCCHESE, "let me know when you boarded". LUCCHESE responded, "im here we just arrived had to charge my phone". DANIYAN then advised LUCCHESE that she will be picked up in the morning. We know that on or about October 18, 2022, LUCCHESE, DANIYAN, and BALOGUN all traveled via airplane to Seattle, Washington for the purpose of committing fraudulent credit union cash withdrawals at DANIYAN's direction. Between October 19 and October 20, 2022, LUCCHESE withdrew a total $29,700 cash in three separate credit union transactions targeting members of

Utah First Credit Union at credit unions in Tukwila, Everett, and Shelton, Washington.

64. Based upon call detail records obtained from T-Mobile, Phone 1B25 received calls or text messages from Phone 1B22 and Phone 1B23. Phone 1B25 sent calls or text messages to Phone 1B23.

Evidence Contained Within Phone 1B22

65. On November 21, 2022, FBI Computer Scientist Alejandro Vargas performed a mobile device extraction of Phone 1B22 and prepared a Cellebrite software report for my forensic review.

66. Evidence obtained from Phone 1B22 established that the phone was used by DANIYAN. This included selfie photographs of DANIYAN, logins to personal accounts, conspirator communications, an activation date following DANIYAN's arrest by Cohoes Police Department, and Internet browser searches for "Cohoes NY Police Station Phone Number."

67. Data on Phone 1B22 shows a conversation on October 17, 2022, wherein DANIYAN instructed an individual from whom DANIYAN purchased fictitious driver's licenses to mail his shipment to "David Daniyan" in Seattle, Washington. During the week of October 17, 2022, DANIYAN was in Seattle, Washington, with BALOGUN and LUCCHESE committing Shared Branching fraudulent cash withdrawals.

68. On multiple occasions in 2022, DANIYAN discussed with ADEKOYA via Phone 1B22's Telegram application sending money to and from DANIYAN's wife's Zelle account. These messages correlated on several

occasions with actual transactions between DANIYAN's spouse and ADEKOYA's spouse. For example, on July 9, 2022, at approximately 16:21 UTC, [redacted] DANIYAN's spouse, transferred $100 via Zelle to A[redacted]O[redacted] ADEKOYA's spouse. At 16:24 UTC, DANIYAN text messaged ADEKOYA via Telegram, "Zelle -ed $100". At 16:37 UTC, ADEKOYA responded to DANIYAN, "Okay". For example, on July 22, 2022, at approximately 2:19 UTC, ADEKOYA text messaged DANIYAN via Telegram, "I'll Zelle your wife now". At 2:32 UTC and 2:33 UTC, respectively, DANIYAN replied to ADEKOYA, "Yes" and "Send it". At 2:44 UTC, [redacted] received $400 from A[redacted]O[redacted] via Zelle transfer.

69. Over 10,000 text messages were recovered from the Telegram application that I have identified as being between DANIYAN and ADEKOYA, discussing in intimate detail the conspiracy at hand. ADEKOYA and DANIYAN collaborated to identify victim credit unions, identify victim customers who banked at those credit unions, recruit bank runners and drivers, order fictitious government identification cards matching victim PII with bank runner's photographs, telephone call credit unions to ascertain Shared Branching restrictions, telephone call credit unions to impersonate victim account holders for the purposes of monitoring account balances and transferring money between accounts, plan travel to credit unions, fraudulently withdraw cash, and divide up the proceeds amongst the conspirators.

70. On June 8, 2022, ADEKOYA sent a series of messages to DANIYAN via Telegram reading, "4 banks in 4-5 states is the best... Workers yapa... Me

and you go make a lot of money... A whole lot. I'll also need your help with coordination... The thing can be overwhelming." DANIYAN replied to ADEKOYA, "Don't worry I'll help you to the fullest." On June 20, 2022, ADEKOYA explained to DANIYAN that credit unions don't vet Shared Branching transactions as thoroughly as they would a non-Shared Branching transaction through a series of Telegram messages reading, "With shared branching it's different... They don't send. It's not their money... If fraud happens they not the one losing so they are more loose with it."

71. Based upon call detail records obtained from T-Mobile, Phone 1B22 received calls or text messages from Phone 1B21. Phone 1B22 sent calls or text messages to Phone 1B21, Phone 1B23, and Phone 1B25.

ADEKOYA and DANIYAN Are the Leaders of the Conspiracy

72. Through my investigation, I have identified ADEKOYA and DANIYAN as the primary architects of the conspiracy. Based on my review of their communications, including those identified and described above, it appears that ADEKOYA has primarily run the planning side of the conspiracy, with DANIYAN providing supervision over the operational aspects of the conspiracy.

73. For example, ADEKOYA appeared to obtain most of the victim PII and usually determined which credit unions would be victimized. On July 16, 2022, ADEKOYA messaged DANIYAN via Telegram, "I mean at this moment to do SS and all those things and to find the banks we gonna do might take me 3-4 days". ADEKOYA frequently complained to DANIYAN about how hard

ADEKOYA was working to plan the fraudulent transactions, that ADEKOYA would spend hours on his laptops conducting research to obtain the PII, and that ADEKOYA had to pay for some of the PII and was short on money.

74. ADEKOYA would frequently call credit unions well in advance of fraudulent activity to ascertain what their financial limit was for Shared Branch cash withdrawals and then locate victim account holders that corresponded with credit unions perceived to have the highest limit. ADEKOYA would often instruct DANIYAN how much to withdraw from the victim's account based on victim account balances. ADEKOYA would obtain the victim account balances by impersonating the victims through their credit union's call center and occasionally transfer funds from the victim's home equity line of credit (HELOC) account into their savings or checking accounts when the credit union did not allow direct cash withdrawals from the HELOCs. Once the money was confirmed to be in the account and ready to withdrawal, ADEKOYA would order DANIYAN to execute the fraudulent transactions.

75. For example, on September 15, 2022, at 21:36 UTC, California Coast Credit Union reported receiving a phone call from telephone number [redacted]3541, impersonating account holder [redacted] The impersonator moved $7,500 from [redacted] HELOC into [redacted] checking account. At 21:36 UTC, ADEKOYA messaged DANIYAN via Telegram stating, "Done... He can go." At 21:44 UTC, P[redacted] entered a Land of Lincoln Credit Union branch located in Decatur, Illinois, presented a fictitious California driver's license identifying

himself as [redacted] and withdrew $7,500 cash from [redacted] account. At 21:47 UTC, DANIYAN messaged ADEKOYA a photograph of the transaction receipt.

76. For example, on October 25, 2022, at 18:06 UTC, DANIYAN messaged ADEKOYA via Telegram, informing him to "Do it now we're 5 minutes away." ADEKOYA replied, "Doing it." At 18:08 UTC, Cyprus Credit Union reported receiving a phone call from phone number [redacted]3105 that impersonated account holder [redacted] to unlawfully access her account. At 18:11 UTC, ADEKOYA informed DANIYAN, "Yea I moved 9900". At 18:15 UTC, BALOGUN dropped LUCCHESE off at an Eglin Federal Credit Union branch located in Niceville, Florida where LUCCHESE unlawfully withdrew $9,900 from [redacted] account. During the transaction, DANIYAN engaged in a 20 minute, 6 second phone call with LUCCHESE. At 18:31 UTC, ADEKOYA appeared to get nervous that the transaction was taking so long. DANIYAN informed ADEKOYA that he was on the phone with LUCCHESE and that LUCCHESE said the transaction was successful. At 18:38 UTC, DANIYAN sent a photograph of the transaction receipt to ADEKOYA.

77. Based on my training and experience, and knowledge of the investigation, the above-communications between ADEKOYA and DANIYAN are consistent with their roles as managers of the overall scheme to defraud.

The Conspiracy Is Ongoing and Has Continued Through 2023

78. Although most of the electronic evidence seized by the FBI spans December 2021 to October 2022, FBI has developed additional evidence that the conspiracy is ongoing, as set forth below.

79. For example, CAPPETTI was transported by JOYNER to credit unions throughout the Northern District of New York and at least the states of Vermont, Massachusetts, Pennsylvania, and Delaware from February to April 2023 for the purposes of committing fraud. After victimizing Corning Credit Union account holders [redacted] on March 9, 2023 via fraudulent cash withdrawals totaling $19,800, CAPPETTI and JOYNER were involved in a traffic stop by the Pennsylvania State Police. The Pennsylvania State Police located two fictitious New Jersey driver's licenses in the name of [redacted] but bearing CAPPETTI's face. Both driver's licenses were accompanied by the fraudulent transaction receipts from Corning Credit Union. Additionally, the driver's licenses were separated into individually marked envelopes with handwritten PII for each victim. The handwriting samples appear to be consistent with numerous handwriting samples belonging to DANIYAN seized by the Cohoes Police Department and located on DANIYAN's electronic devices, indicating that DANIYAN had supplied CAPPETTI with at least the PII necessary to effect the fraudulent withdrawals.

80. Additionally, ADEKOYA was identified as a suspect by the Calhoun County Sheriff's Office in Alabama following a string of fraudulent activity in Alabama and Georgia in September 2023. On September 15, 2023, H[redacted] G[redacted] entered three separate Family Savings Credit Union locations in eastern Alabama and withdrew a total of $29,350 from three separate credit union customers' accounts. Staff members from Family Savings Credit Union provided a partial identification of the vehicle that had been dropping G[redacted]

off around the credit union branches. Through a collaboration of Calhoun County Sheriff's Office detectives and Oxford Police Department detectives, surveillance camera footage was reviewed from a dental office and a license plate reader software program to identify the suspect vehicle as a white Chevrolet Malibu bearing Florida registration [redacted]

81. Calhoun County Sheriff's Office determined that the vehicle was rented by Avis on September 13, 2023, at approximately 11:05 A.M., at the Greenville-Spartanburg International Airport in South Carolina by ADEKOYA. The vehicle was returned to Avis on September 15, 2023 at approximately 6:00 P.M. at the Birmingham-Shuttlesworth International Airport in Birmingham, Alabama. Additionally, ADEKOYA rented a white Ford Expedition from Avis at the Hartsfield-Jackson Atlanta International Airport in Georgia on September 21, 2023 at approximately 9:54 A.M. G[redacted] was arrested by the Morrow Police Department in Georgia on September 22, 2023 at approximately 3:07 P.M. after fraudulently withdrawing $9,700 cash from an iThink Financial Credit Union customer's account. ADEKOYA returned the rental car on September 22, 2023 at approximately 6:00 P.M. at the same location.

82. After waiver of her *Miranda* rights, G[redacted] was interviewed by Calhoun County Sheriff's Office detectives while incarcerated at the Bartow County Jail in Georgia. G[redacted] advised that she was recruited to commit fraud while panhandling outside of a McDonald's in northern New Jersey in July 2023. G[redacted] was provided food, clothing, a phone, and was introduced to an individual called "Sammy." G[redacted] identified "Sammy" as ADEKOYA

when presented with a photo lineup prepared by the investigators. G[redacted] advised that she was flown to a southern state to commit fraud and was picked up in a rental vehicle by ADEKOYA. G[redacted] admitted to being driven by ADEKOYA throughout Alabama and Georgia to commit fraud in September 2023. Following G[redacted] arrest on September 22, 2023, she flew back to New Jersey and attempted to avoid contact with ADEKOYA. However, ADEKOYA located G[redacted] at her hotel room and questioned G[redacted] about her contact with law enforcement to determine whether or not he was a subject of interest.

83. G[redacted] also recalled ADEKOYA operating a black-colored car on October 14, 2023 between 10:00 AM and 11:00 AM when she met ADEKOYA at an Enterprise rental car facility in Fairlawn, New Jersey. ADEKOYA was going to provide G[redacted] with money to rent a vehicle so that G[redacted] could drive to Mississippi to commit more fraud, but G[redacted] was unable to rent the vehicle that day. On October 16, 2023, between 11:00 AM and 12:00 PM, ADEKOYA again met G[redacted] across the street from Enterprise. This time, G[redacted] reported ADEKOYA was driving a white-colored Mercedes-Benz SUV. Based on my training and experience and knowledge of the investigation, I believe ADEKOYA was driving the GLE.

84. Financial records obtained by the FBI indicate that the relationship between DANIYAN and ADEKOYA continued throughout 2023. For example, between at least January 5, 2023 and July 6, 2023, [redacted] TD Bank account ending in [redacted] was used to transfer at least $4,200 to A[redacted] C[redacted] JPMorgan Chase Bank account ending in [redacted] In addition,

between at least March 1, 2023 and April 21, 2023, A[redacted] O[redacted] JPMorgan Chase Bank account ending in [redacted] was used to transfer at least $2,640 to [redacted] TD Bank account ending in [redacted] Additionally, on March 1, 2023, A[redacted] O[redacted] Zelle account was used to transfer $1,000 to [redacted] Zelle account. [redacted] Zelle account was then used to transfer $1,000 to Jerjuan JOYNER's Zelle account on the same day. This transfer occurred approximately one week prior to JOYNER transporting CAPPETTI to Corning Credit Union to commit fraud. As previously established in this warrant affidavit, DANIYAN and ADEKOYA are banking in their spouse's names, and these transactions are consistent with the financial transactions between the spouses during the period we have obtained communications between DANIYAN and ADEKOYA.

85. In my training and experience, and given my knowledge of the investigation, these transactions, combined with ADEKOYA's recent bank fraud activity, establish that DANIYAN and ADEKOYA are still engaged in an ongoing conspiracy aimed at defrauding financial institutions.

[redacted] is ADEKOYA's Residence

86. As set forth below, [redacted] has been ADEKOYA's residence from at least February 2020 through the present. Accordingly, ADEKOYA has lived at the residence throughout the entire time-period of the crimes under investigation.

87. ADEKOYA has been the registered occupant and billing recipient of [redacted] from February 1, 2020 to present time with the electric

company [redacted] In October 2023, ADEKOYA paid down his electric bill debt with [redacted] from $4,031.21 to $748.20.

88. On November 30, 2023, FBI obtained confirmation from [redacted] management that ADEKOYA and O[redacted] continue to reside in [redacted] and renewed their lease for that unit on February 3, 2023 for a period of 12 months.

89. Based on information provided by Federal Express, ADEKOYA appeared to receive a shipment on November 3, 2022, from a known vendor of fictitious government identifications to [redacted].

90. On July 17, 2023, at approximately 10:56 AM, Agents from FBI Newark surveilled ADEKOYA departing the underground parking garage beneath [redacted] in the C300.

91. Additionally, A[redacted] T[redacted] O[redacted] known to be ADEKOYA's spouse, opened a TD Bank account ending in [redacted] on August 15, 2022 and listed [redacted] as her address. As of October 25, 2023, [redacted] was still linked to this account and this account was actively being used by both O[redacted] and ADEKOYA.

92. On November 28, 2023, a United States Postal Inspection Services ("USPIS") address check performed by Postal Inspector Timothy Maloney on [redacted] confirmed the address is registered for mail purposes to ADEKOYA and A[redacted] T. O[redacted]

ADEKOYA OWNS AND USES THE C300

93. ADEKOYA has been established as the owner and operator of the C300 through documentary evidence and surveillance.

94. Capital One Auto Finance records indicate that ADEKOYA was the purchaser and is the titled owner of the C300. During the analyzed timeframe of known fraudulent activity as part of this conspiracy, ADEKOYA and/or ADEKOYA's spouse paid approximately $7,682.40 to Capital One Auto Finance as the lienholder on the C300, through monthly payments of $382.12. Many of the monthly payments toward this vehicle were preceded by suspicious large dollar cash deposits into the bank accounts from which the payments were made. For example, between April 10 and April 12, 2022, $11,8000 cash was deposited into ADEKOYA's spouse's JPMorgan Chase bank account ending in 8717 from two separate ATMs. On April 12, 2022, ADEKOYA's monthly car payment of $382.12 is made from this account.

95. Surveillance footage from a TD Bank branch ATM located at [redacted] Fort Lee, NJ on Monday, June 26, 2023, showed ADEKOYA pull up to the ATM in a black-colored Mercedes Benz with a large stack of $100 bills in his hand. A female was seated in the passenger's seat at the time. ADEKOYA appeared to deposit the money into the ATM, corresponding with a $5,300 cash deposit into TD Bank account ending in 3814 from an ATM at that location on that day. Based on my training and experience, and knowledge of the investigation, ADEKOYA was driving the C300 on that date.

96. On July 17, 2023, at approximately 10:56 AM, Agents from FBI Newark surveilled ADEKOYA departing the underground parking garage beneath [redacted] in the C300. ADEKOYA drove to the [redacted] located at [redacted], New Jersey, where ADEKOYA and his spouse exited the vehicle and went inside. ADEKOYA also drove to Trader Joe's, Target, Home Goods, Smoke Shop, Food Bazaar, and Chase Bank before returning to the [redacted]g garage.

ADEKOYA LEASES AND USES THE GLE

97. Mercedes-Benz Financial Services records show ADEKOYA as the purchaser and lessee of the GLE. The New Jersey Motor Vehicle Commission concurrently lists ADEKOYA as the registered lessee of this vehicle. During the analyzed timeframe of known fraudulent activity as part of this conspiracy, ADEKOYA and/or ADEKOYA's spouse paid approximately $49,756.91 to Mercedes-Benz Financial Services as part of the lease agreement through monthly payments of $2,257.17. Many of the monthly payments toward this vehicle were preceded by suspicious large dollar cash deposits into the bank accounts from which the payments were made. For example, on May 15, 2022, $6,000 cash was deposited into ADEKOYA's wife's JPMorgan Chase bank account ending in [redacted] from which ADEKOYA made a two-month car payment of $4,514.34 on May 17, 2022.

98. Benz Financial Services records show ADEKOYA as the purchaser and lessee of the GLE. The New Jersey Motor Vehicle Commission concurrently lists ADEKOYA as the registered lessee of this vehicle. During the

analyzed timeframe of known fraudulent activity as part of this conspiracy, ADEKOYA and/or ADEKOYA's spouse paid approximately $49,756.91 to Mercedes-Benz Financial Services as part of the lease agreement through monthly payments of $2,257.17. Many of the monthly payments toward this vehicle were preceded by suspicious large dollar cash deposits into the bank accounts from which the payments were made. For example, on May 15, 2022, $6,000 cash was deposited into ADEKOYA's wife's JPMorgan Chase bank account ending in [redacted] from which ADEKOYA made a two-month car payment of $4,514.34 on May 17, 2022.

99. In addition, on August 12, 2022, $4,000 cash was deposited into ADEKOYA's wife's JPMorgan Chase bank account ending in [redacted] from which ADEKOYA's monthly car payment of $2,257.17 was made on August 13, 2022. Likewise, on July 14, 2023, $2,600 cash was deposited into ADEKOYA's wife's TD Bank account ending in [redacted] from which ADEKOYA's monthly car payment of $2,257.17 was made on July 17, 2023.

100. Surveillance footage from a TD Bank branch ATM located at [redacted], Fort Lee, NJ on Saturday, August 12, 2023, showed ADEKOYA pull up to the ATM in a white Mercedes-Benz GLE and exit the vehicle with a large stack of one-hundred-dollar bills in his hand. ADEKOYA tucked the stack of bills under his chin as he manipulated the buttons on the ATM. On August 14, 2023, ADEKOYA's spouse's TD Bank account ending in [redacted] posted $8,900 cash deposited from that location. Based on my training

and experience, and knowledge of the investigation, ADEKOYA was driving the GLE on that date.

Retention of Records of Fraudulent Activity

101. Based on my training, experience, and knowledge of the investigation, there is probable cause to believe that ADEKOYA has committed the Subject Offenses and evidence, fruits, and instrumentalities of the Subject Offenses is likely to be found in ADEKOYA's residence, his vehicles, and on his person. This is in part because those who engage in fraud and identity theft-related crimes frequently use the internet, computers, cell phones, and other electronic devices to research, plan, and execute their crimes. As set forth above, ADEKOYA has used electronic devices to research, plan, and execute the Subject Offenses. Other members of the conspiracy have likewise used phones, including multiple devices, or "burner phones," to perpetrate and orchestrate the Subject Offenses. Fraudsters, like every other person, typically keep such electronic devices in their homes, vehicles, and/or on their person.

102. Based on my training and experience, I know there are certain characteristics common to individuals who engage in fraud, specifically:

a. Persons engaged in fraud frequently retain records of their transactions within their residence, place of business, rented storage units, vehicles, or other places under their control, including on their person and within their personal belongings. These records may be in the form of written notes and email correspondence, receipts, negotiated instruments, contracts, bank statements, and

other records. Records of this kind are also often stored on computer media including phones.

b. Persons engaged in fraud often maintain such records for long periods of time, particularly when they are involved in ongoing criminal conduct over a long period of time. Although this is true for paper records, it is especially true for records kept in digital format. Digital storage does not require physical storage space and because digital storage space, whether in the form of computer hard drives, external hard drives, flash memory, digital video disks, compact disks, or other forms of digital storage media, is inexpensive, and easy to purchase and maintain, it is not uncommon for persons engaged in long-term financial crimes to maintain records in both paper and digital format for a number of years. There are many reasons why criminal offenders maintain evidence for long periods of time. The evidence may be innocuous at first glance (e.g. location information, financial, credit card, and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, checkbooks, video recordings and photographs, utility records, ownership records, letters and notes, and financial records, escrow files, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and software), but have significance and relevance when considered in light of other evidence.

c. Those engaged in fraud and identity theft typically engage in financial transactions with the fruits of their crimes, resulting in banking and financial records that contain evidence of the flow of criminal proceeds, the location of criminal proceeds, and the means by which the perpetrators transmit criminal proceeds. In this case, the criminal proceeds were initially withdrawn in cash. In my training and experience, individuals engaged in fraud typically maintain proceeds in the form of cash for extended periods of time. Cash is highly fungible and therefore difficult to trace.

103. In this case, ADEKOYA has resided at [redacted] since at least February 2020 to the present. Accordingly, he has resided in that residence for the entire time-period of this ongoing nationwide bank fraud conspiracy he has played a significant role in perpetrating. He has had records, such as those sought in these warrants, in his possession as evidenced by his communications with DANIYAN as described above. In my training and experience, based on the foregoing, it is highly likely that ADEKOYA maintains the evidence, fruits, and instrumentalities of his crimes at his residence, in the vehicles he operates, and on his person, as set forth in Attachments B-1 through B-4.

TECHNICAL TERMS

104. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

105. As described above and in Attachments B-1 through B-4, this application seeks permission to search for records that might be found in [redacted], the C300, the GLE, and on the person of ADEKOYA, in

whatever form they are found. One form in which the records might be found is data stored on a cell phone, tablet, computer's hard drive or other storage media. Thus, the warrants applied for would authorize the seizure of electronic devices or, potentially, the copying of electronically stored information, subject to the parameters set forth below, all under Rule 41(e)(2)(B).

106. In my training and experience, couples who reside together in the same residence often share computer equipment, such as computers, laptops, tablets, and electronic storage media ("SHARED COMPUTER EQUIPMENT"). SHARED COMPUTER EQUIPMENT is typically found in common areas of a residence, as opposed to bedrooms or areas typically used by specific members of a family. Typically, such equipment is not labeled as belonging to any particular person. For example, a school- or work-issued laptop will usually bear an identification marker identifying it as such. SHARED COMPUTER EQUIPMENT typically does not bear any such identification.

107. Cellular phones, unlike SHARED COMPUTER EQUIPMENT, are typically only used by one person. However, in my training and experience, individuals who utilize multiple cellular phones, or "burner phones," in connection with criminal activity often maintain many such devices. It is common for family members to be unfamiliar with any particular such device, such that a family member – even one living in the same household or utilizing shared vehicles – may be unable to identify such a device as belonging to the criminal. Commonly, such family members are unfamiliar with a burner device

and may be unable to identify the device as belonging to anyone within the household.

108. It is possible that [redacted], the C300, or the GLE will contain electronic devices that are predominately used, and perhaps owned, by persons as to whom there is not evidence of criminal conduct. To narrowly tailor the scope of any search and seizure, the applied-for warrant would allow the seizure and search of only SHARED COMPUTER EQUIPMENT found in common areas of [redacted] as well as anywhere in the C300 and GLE reasonably believed to be used, possessed, or accessed by ADEKOYA and SHARED COMPUTER EQUIPMENT and cellular phones: (1) found on the person of, or within reasonable proximity of ADEKOYA; (2) found within a bedroom where ADEKOYA is determined to have been sleeping; (3) attributed to ADEKOYA using biometric unlocking information described below; (4) identified as belonging to ADEKOYA if a law enforcement agent observes an electronic device to ring, vibrate or otherwise indicate receipt of an incoming call when called by a law enforcement agent; (5) identified by ADEKOYA or A[redacted] O[redacted] as belonging to ADEKOYA; or (6) which ADEKOYA or A[redacted] A[redacted] are able to identify as belonging to any specific member of the household.

109. *Probable cause.* I submit that if an electronic device within the scope of the proposed warrants is located, there is probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses, as set forth

in Attachments B-1 through B-4, will be stored on such electronic devices, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations,

artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of other evidence related to this investigation, including financial records, receipts, and invoices, I am aware that computer equipment was used to generate, store, and print documents used in the Subject Offenses. There is reason to believe that there are computer systems currently located at the properties to be searched and on the person of ADEKOYA, at least in the form of cellular phones or other small portable electronic devices.

110. *Forensic evidence.* As further described in Attachments B-1 through B-4, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer, cell

phone, tablet, or storage medium located in the properties to be searched or on the person of ADEKOYA because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information

stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the

suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to access bank accounts, shipment records, and other financial information, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of

committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

111. *Necessity of seizing or copying entire computers, cell phones, tablets, or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires

considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

112. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging,

or otherwise copying computers, cell phones, tablets, and storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

113. *Biometric unlocking of devices.* The warrants I am applying for would permit law enforcement to obtain from ADEKOYA the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For

example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by

entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4

hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the properties to be searched, and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of ADEKOYA to the fingerprint scanner of the device; (2) hold the device in front of the face of ADEKOYA and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

114. Based on the foregoing, I respectfully request that the Court issue the applied-for search warrants.

REQUEST FOR SEALING

115. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Attested to by the affiant.

Respectfully submitted,

Spenser Warren
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone, this __8th___ day of December.

Jose R. Almonte @ 4:02 PM

Honorable José R. Almonte
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

Property to be Searched

1. The property to be searched is [redacted], New Jersey 07010 [redacted] and includes any garage space or storage unit under the control of or used by Oluwaseun ADEKOYA at [redacted] New Jersey 07010 and any open or closed containers therein. [redacted] is located within [redacted], which is a high-rise luxury apartment rental community that offers approximately 314 separate studio, one, and two bedroom apartments for lease. The building appears to be approximately 15 stories tall with 24-hour security, a rooftop pool, a grand plaza with restaurants and retail stores, a fitness center, a lounge, and an underground parking garage, per the property's website. Based on publicly accessible floor plans, [redacted] likely contains a living room, a kitchen, a laundry room, closet space, at least one bedroom, and at least one bathroom. A photograph of [redacted]

ATTACHMENT B-1

Items to be Seized

1. All evidence, fruits, and instrumentalities of the crimes of conspiracy to commit bank fraud, in violation of 18 U.S.C. §§ 1349 and 1344 and aggravated identity theft, in violation of 18 U.S.C. § 1028A (aggravated identity theft) (the "Subject Offenses"), involving Oluwaseun ADEKOYA, and any co-conspirators known and unknown, covering the time period of January 1, 2021 to present unless otherwise indicated, including:

a. Evidence concerning occupancy or ownership of [redacted], New Jersey 07010, a 2016 black Mercedes-Benz C300 bearing [redacted], and a 2021 white Mercedes-Benz GLE bearing [redacted], including utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, invoices, registration documents, identification documents, address books, and telephone directories.

b. Evidence concerning aliases or identities used by Oluwaseun ADEKOYA, including identification instruments and documents, financial records, telephone bills, legal records, and other documentation indicating the use by ADEKOYA of a name or identity other than ADEKOYA.

c. Evidence concerning the identity or location of, and communications with, suspects, coconspirators, and bank fraud or identity theft victims.

d. Records related to personal identifying information ("PII") of anyone other than ADEKOYA or his spouse, A[redacted]T[redacted] O[redacted]

e. Records related to credit unions or banks, to include locations, account numbers, participation in shared branching, shared branching transaction limitations.

f. Records related to fraudulent banking transactions conducted in the name of customers, including location information, branch information, transaction amounts, identity of individuals conducting the transactions or in whose name the transactions were conducted, and time and date of transaction.

g. Any and all financial and wealth information for ADEKOYA, including but not limited to bank account records, bank statements, deposit slips, ATM withdrawal slips, cancelled checks, check registers, withdrawal slips, wire and inter-account transfers, cryptocurrency transfers, cashier's checks, money orders, signature cards, mutual fund and other securities records, credit applications, loan documents and loan payments records, debit cards, credit cards, credit card statements, credit card account applications, invoices, vendor

payments, subcontractor invoices, insurance records, deeds, titles, receipts and/or bills evidencing cash expenditures.

h. Records related to the acquisition or purchase of customer financial information, PII, and fake identifications.

i. Evidence of the disposition of proceeds of the Subject Offenses, including U.S. currency, foreign currency, cryptocurrency, jewelry, precious metals, other valuables, pre-paid debit cards, financial instruments, and financial accounts constituting or traceable to the proceeds of the Subject Offenses, and including any passwords, passphrases, public or private keys, physical devices, physical keys, and cryptocurrency recover mnemonics needed by law enforcement to access such items.

j. Records and communications relating to the storage of items, records or documents at any other location, including but not limited to contracts and lease agreements for offices, storage units or safe deposit boxes. Keys and other access devices for storage units, safe deposit boxes, vehicles, and other closed containers.

k. Photographs and communications related to the crimes under investigation and identifying victims, coconspirators, or other evidence of criminal activity.

2. The items to be seized include any computer devices, cellular phones, and storage media reasonably believed to contain any electronically

stored information falling within the categories set forth in this Attachment B-1, above. The electronic devices to be seized are limited to desktop computers, laptop computers, tablets, and external storage media ("SHARED COMPUTER EQUIPMENT") found in common areas of [redacted] reasonably believed to be used, possessed, or accessed by ADEKOYA, and SHARED COMPUTER EQUIPMENT and cellular phones: (1) found on the person of, or within reasonable proximity of ADEKOYA; (2) found within a bedroom where ADEKOYA is determined to have been sleeping; (3) attributed to ADEKOYA using biometric unlocking information described below; (4) identified as belonging to ADEKOYA if a law enforcement agent observes an electronic device to ring, vibrate or otherwise indicate receipt of an incoming call when called by a law enforcement agent; (5) identified by ADEKOYA or A[redacted]O[redacted]as belonging to ADEKOYA; or (6) which ADEKOYA or A[redacted]A[redacted]are able to identify as belonging to any specific member of the household.

3. For any computer or storage medium, to include desktop and laptop computers, tablets, disk drives, modems, thumb drives, personal digital assistants, cellular phones, digital cameras, and scanners, whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration

files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

6. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

7. During the execution of the search, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of ADEKOYA to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face of ADEKOYA and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

8. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT A-2

Property to be Searched

1. The property to be searched is a 2016 black Mercedes-Benz C300 bearing [redacted] (the "C300").

ATTACHMENT B-2

Items to be Seized

1. All evidence, fruits, and instrumentalities of the crimes of conspiracy to commit bank fraud, in violation of 18 U.S.C. §§ 1349 and 1344 and aggravated identity theft, in violation of 18 U.S.C. § 1028A (aggravated identity theft) (the "Subject Offenses"), involving Oluwaseun ADEKOYA, and any co-conspirators known and unknown, covering the time period of January 1, 2021 to present unless otherwise indicated, including:

a. Evidence concerning occupancy or ownership of [redacted] New Jersey 07010, a 2016 black Mercedes-Benz C300 bearing [redacted], and a 2021 white Mercedes-Benz GLE bearing [redacted], including utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, invoices, registration documents, identification documents, address books, and telephone directories.

b. Evidence concerning aliases or identities used by Oluwaseun ADEKOYA, including identification instruments and documents, financial records, telephone bills, legal records, and other documentation indicating the use by ADEKOYA of a name or identity other than ADEKOYA.

c. Evidence concerning the identity or location of, and communications with, suspects, coconspirators, and bank fraud or identity theft victims.

d. Records related to personal identifying information ("PII") of anyone other than ADEKOYA or his spouse, A[redacted] T[redacted] C[redacted]

e. Records related to credit unions or banks, to include locations, account numbers, participation in shared branching, shared branching transaction limitations.

f. Records related to fraudulent banking transactions conducted in the name of customers, including location information, branch information, transaction amounts, identity of individuals conducting the transactions or in whose name the transactions were conducted, and time and date of transaction.

g. Any and all financial and wealth information for ADEKOYA, including but not limited to bank account records, bank statements, deposit slips, ATM withdrawal slips, cancelled checks, check registers, withdrawal slips, wire and inter-account transfers, cryptocurrency transfers, cashier's checks, money orders, signature cards, mutual fund and other securities records, credit applications, loan documents and loan payments records, debit cards, credit cards, credit card statements, credit card account applications, invoices, vendor

payments, subcontractor invoices, insurance records, deeds, titles, receipts and/or bills evidencing cash expenditures.

h. Records related to the acquisition or purchase of customer financial information, PII, and fake identifications.

i. Evidence of the disposition of proceeds of the Subject Offenses, including U.S. currency, foreign currency, cryptocurrency, jewelry, precious metals, other valuables, pre-paid debit cards, financial instruments, and financial accounts constituting or traceable to the proceeds of the Subject Offenses, and including any passwords, passphrases, public or private keys, physical devices, physical keys, and cryptocurrency recover mnemonics needed by law enforcement to access such items.

j. Records and communications relating to the storage of items, records or documents at any other location, including but not limited to contracts and lease agreements for offices, storage units or safe deposit boxes. Keys and other access devices for storage units, safe deposit boxes, vehicles, and other closed containers.

k. Photographs and communications related to the crimes under investigation and identifying victims, coconspirators, or other evidence of criminal activity.

2. The items to be seized include any computer devices, cellular phones, and storage media reasonably believed to contain any electronically

stored information falling within the categories set forth in this Attachment B-2 above, including, but not limited to, desktop and laptop computers, tablets, disk drives, thumb drives, personal digital assistants, cellular phones, digital cameras, and portable scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review. The items to be seized include any cellular telephones that belong to ADEKOYA or are reasonably believed to have been used by ADEKOYA in connection with the Subject Offenses.

3. For any computer or storage medium, to include desktop and laptop computers, tablets, disk drives, modems, thumb drives, personal digital assistants, cellular phones, digital cameras, and scanners, whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or

absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and

cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

6. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

7. During the execution of the search, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of ADEKOYA to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face of ADEKOYA and activate the facial recognition feature, for the

purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

8. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT A-3

Property to be Searched

1. The property to be searched is a 2021 white Mercedes-Benz GLE bearing [redacted].

ATTACHMENT B-3

Items to be Seized

1. All evidence, fruits, and instrumentalities of the crimes of conspiracy to commit bank fraud, in violation of 18 U.S.C. §§ 1349 and 1344 and aggravated identity theft, in violation of 18 U.S.C. § 1028A (aggravated identity theft) (the "Subject Offenses"), involving Oluwaseun ADEKOYA, and any co-conspirators known and unknown, covering the time period of January 1, 2021 to present unless otherwise indicated, including:

a. Evidence concerning occupancy or ownership of [redacted] New Jersey 07010, a 2016 black Mercedes-Benz C300 bearing [redacted], and a 2021 white Mercedes-Benz GLE bearing [redacted], including utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, invoices, registration documents, identification documents, address books, and telephone directories.

b. Evidence concerning aliases or identities used by Oluwaseun ADEKOYA, including identification instruments and documents, financial records, telephone bills, legal records, and other documentation indicating the use by ADEKOYA of a name or identity other than ADEKOYA.

c. Evidence concerning the identity or location of, and communications with, suspects, coconspirators, and bank fraud or identity theft victims.

d. Records related to personal identifying information ("PII") of anyone other than ADEKOYA or his spouse, A[redacted]T[redacted] O[redacted]

e. Records related to credit unions or banks, to include locations, account numbers, participation in shared branching, shared branching transaction limitations.

f. Records related to fraudulent banking transactions conducted in the name of customers, including location information, branch information, transaction amounts, identity of individuals conducting the transactions or in whose name the transactions were conducted, and time and date of transaction.

g. Any and all financial and wealth information for ADEKOYA, including but not limited to bank account records, bank statements, deposit slips, ATM withdrawal slips, cancelled checks, check registers, withdrawal slips, wire and inter-account transfers, cryptocurrency transfers, cashier's checks, money orders, signature cards, mutual fund and other securities records, credit applications, loan documents and loan payments records, debit cards, credit cards, credit card statements, credit card account applications, invoices, vendor

payments, subcontractor invoices, insurance records, deeds, titles, receipts and/or bills evidencing cash expenditures.

h. Records related to the acquisition or purchase of customer financial information, PII, and fake identifications.

i. Evidence of the disposition of proceeds of the Subject Offenses, including U.S. currency, foreign currency, cryptocurrency, jewelry, precious metals, other valuables, pre-paid debit cards, financial instruments, and financial accounts constituting or traceable to the proceeds of the Subject Offenses, and including any passwords, passphrases, public or private keys, physical devices, physical keys, and cryptocurrency recover mnemonics needed by law enforcement to access such items.

j. Records and communications relating to the storage of items, records or documents at any other location, including but not limited to contracts and lease agreements for offices, storage units or safe deposit boxes. Keys and other access devices for storage units, safe deposit boxes, vehicles, and other closed containers.

k. Photographs and communications related to the crimes under investigation and identifying victims, coconspirators, or other evidence of criminal activity.

2. The items to be seized include any computer devices, cellular phones, and storage media reasonably believed to contain any electronically

stored information falling within the categories set forth in this Attachment B-3 above, including, but not limited to, desktop and laptop computers, tablets, disk drives, thumb drives, personal digital assistants, cellular phones, digital cameras, and portable scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review. The items to be seized include any cellular telephones that belong to ADEKOYA or are reasonably believed to have been used by ADEKOYA in connection with the Subject Offenses.

3. For any computer or storage medium, to include desktop and laptop computers, tablets, disk drives, modems, thumb drives, personal digital assistants, cellular phones, digital cameras, and scanners, whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or

absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and

cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

6. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

7. During the execution of the search, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of ADEKOYA to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face of ADEKOYA and activate the facial recognition feature, for the

purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

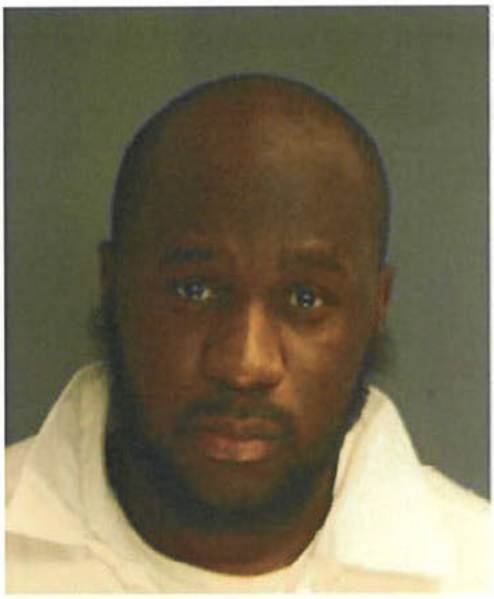
8. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT A-4

Person to be Searched

1. This warrant authorizes the search of the person of Oluwaseun ADEKOYA, date of birth [redacted] wherever he is found within the District of New Jersey, as well as anything he is carrying or holding (e.g. backpack, bag, briefcase) when law enforcement encounters him. ADEKOYA is approximately 6 feet tall, weighing approximately 190 pounds. ADEKOYA has brown eyes, black hair, and a dark skin complexion. He is pictured below:

Surveillance photograph 7/17/23



Prison photograph approximately 2017

ATTACHMENT B-4

Items to be Seized

1. All evidence, fruits, and instrumentalities of the crimes of conspiracy to commit bank fraud, in violation of 18 U.S.C. §§ 1349 and 1344 and aggravated identity theft, in violation of 18 U.S.C. § 1028A (aggravated identity theft) (the "Subject Offenses"), involving Oluwaseun ADEKOYA and any co-conspirators known and unknown, covering the time period of January 1, 2021 to present unless otherwise indicated, including:

a. Evidence concerning occupancy or ownership of [redacted] New Jersey 07010, a 2016 black Mercedes-Benz C300 bearing [redacted], and a 2021 white Mercedes-Benz GLE bearing [redacted], including utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, invoices, registration documents, identification documents, address books, and telephone directories.

b. Evidence concerning aliases or identities used by Oluwaseun ADEKOYA, including identification instruments and documents, financial records, telephone bills, legal records, and other documentation indicating the use by ADEKOYA of a name or identity other than ADEKOYA.

c. Evidence concerning the identity or location of, and communications with, suspects, coconspirators, and bank fraud or identity theft victims.

d. Records related to personal identifying information ("PII") of anyone other than ADEKOYA or his spouse, A[redacted] T[redacted] O[redacted]

e. Records related to credit unions or banks, to include locations, account numbers, participation in shared branching, shared branching transaction limitations.

f. Records related to fraudulent banking transactions conducted in the name of customers, including location information, branch information, transaction amounts, identity of individuals conducting the transactions or in whose name the transactions were conducted, and time and date of transaction.

g. Any and all financial and wealth information for ADEKOYA, including but not limited to bank account records, bank statements, deposit slips, ATM withdrawal slips, cancelled checks, check registers, withdrawal slips, wire and inter-account transfers, cryptocurrency transfers, cashier's checks, money orders, signature cards, mutual fund and other securities records, credit applications, loan documents and loan payments records, debit cards, credit cards, credit card statements, credit card account applications, invoices, vendor

payments, subcontractor invoices, insurance records, deeds, titles, receipts and/or bills evidencing cash expenditures.

h. Records related to the acquisition or purchase of customer financial information, PII, and fake identifications.

i. Evidence of the disposition of proceeds of the Subject Offenses, including U.S. currency, foreign currency, cryptocurrency, jewelry, precious metals, other valuables, pre-paid debit cards, financial instruments, and financial accounts constituting or traceable to the proceeds of the Subject Offenses, and including any passwords, passphrases, public or private keys, physical devices, physical keys, and cryptocurrency recover mnemonics needed by law enforcement to access such items.

j. Records and communications relating to the storage of items, records or documents at any other location, including but not limited to contracts and lease agreements for offices, storage units or safe deposit boxes. Keys and other access devices for storage units, safe deposit boxes, vehicles, and other closed containers.

k. Photographs and communications related to the crimes under investigation and identifying victims, coconspirators, or other evidence of criminal activity.

2. The items to be seized include any computer devices, cellular phones, and storage media reasonably believed to contain any electronically

stored information falling within the categories set forth in this Attachment B-4 above, including, but not limited to, desktop and laptop computers, tablets, disk drives, thumb drives, personal digital assistants, cellular phones, digital cameras, and portable scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review. The items to be seized include any cellular telephones that belong to ADEKOYA or are reasonably believed to have been used by ADEKOYA in connection with the Subject Offenses.

3. For any computer or storage medium, to include desktop and laptop computers, tablets, disk drives, modems, thumb drives, personal digital assistants, cellular phones, digital cameras, and scanners, whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or

absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and

cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

6. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

7. During the execution of the search, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of ADEKOYA to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face of ADEKOYA and activate the facial recognition feature, for the

purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

8. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.